Order No. 829 Citation	Directive / Guidance	Resolution
P 43	[the Commission directs] that NERC, pursuant to section 215(d)(5) of the FPA, develop a forward-looking, objective-driven new or modified Reliability Standard to require each affected entity to develop and implement a plan that includes security controls for supply chain management for industrial control system hardware, software, and services associated with bulk electric system operations.	Proposed CIP-013-1 addresses the directive. The purpose of the proposed standard is: *To mitigate cyber security risks to the reliable operation of the Bulk Electric System (BES) by implementing security controls for supply chain risk management of BES Cyber Systems.* CIP-013-1 is applicable to high and medium impact BES Cyber Systems. The proposed applicability appropriately focuses industry resources on supply chain cyber security risk management for industrial control system hardware, software, and computing and networking services associated with BES operations.
P 44	[the Commission directs] NERC to submit the new or modified Reliability Standard within one year of the effective date of this Final Rule. NERC should submit an informational filing [by December 26, 2016] with a plan to address the Commission's directive.	The proposed/modified standard(s) must be filed by September 27, 2017. NERC filed its plan to address the directive on December 15, 2016.
P 45	The plan required by the new or modified Reliability Standard developed by NERC should address, at a minimum, the following four specific security objectives in the context of addressing supply chain management risks: (1) software integrity and authenticity; (2) vendor remote access; (3) information system planning; and (4) vendor risk management and procurement controls. Responsible entities should be required to achieve these four objectives but have the flexibility as to how to reach the objective (i.e., the Reliability Standard should set goals (the	The directive is addressed by Requirements R1, ~~R3~~R2, ~~R4,~~ and ~~R5~~ R3 of proposed CIP-013-1. Requirement R1 specifies that entities must ~~implement~~ develop, and Requirement R2 specifies that entities must implement, one or more documented supply chain cyber security risk management plan(s) for high and medium impact BES Cyber Systems that ~~address~~ include one or more

Order No. 829 Citation	Directive / Guidance	Resolution
	"what"), while allowing flexibility in how a responsible entity subject to the Reliability Standard achieves that goal (the "how")).	process(es)~~controls~~ for mitigating cyber security risks to BES Cyber Systems ~~and, if applicable, associated Electronic Access Control or Monitoring Systems, Physical Access Control Systems, and Protected Cyber Assets~~. The plans address the four objectives from Order No. 829 (P 45) during the planning, acquisition, and deployment phases of the system life cycle. ~~Requirements R3 through R5 address controls for software integrity and authenticity and vendor remote access that apply to the operate/maintain phase of the system life cycle as described further below.~~ **Proposed CIP-013-1 Requirement R1** **R1.** Each Responsible Entity shall ~~implement~~ develop one or more documented supply chain cyber security risk management plan(s) for high and medium impact BES Cyber Systems. ~~that address controls for mitigating cyber security risks to BES Cyber Systems and, if applicable, associated Electronic Access Control or Monitoring Systems, Physical Access Control Systems, and Protected Cyber Assets.~~ The plan(s) shall ~~address~~include: ~~**1.1.**~~ One or more process(es) used in planning for the procurement of BES Cyber Systems to identify and assess cyber security risk(s) to the Bulk Electric System from vendor products or services resulting from: (i) procuring and installing vendor equipment and software; and (ii) transitions from one vendor(s) to another

Order No. 829 Citation	Directive / Guidance	Resolution
		vendor(s)~~One or more process(es) used The use of controls in planning for the procurement of BES Cyber Systems to identify and assess cyber security risk(s) to the Bulk Electric System from vendor products or services resulting from: (i) procuring and installing vendor equipment and software; (ii) network architecture security; and (iii) transitions from one vendor(s) to another vendor(s). planning and development to:~~ ~~**1.2.** Identify and assess risk(s) during the procurement and deployment of vendor products and services; and~~ ~~**1.3.**1.1. Evaluate methods to address identified risk(s).~~ ~~**1.4.**1.2. One or more process(es) used in procuring BES Cyber Systems ~~The use of controls in procuring vendor product(s) or service(s)~~ that address the following, as applicable~~ items, to the extent each item applies to the Responsible Entity's BES Cyber Systems and, if applicable, associated Electronic Access Control or Monitoring Systems, Physical Access Control Systems, and Protected Cyber Assets~~: **1.2.1.** ~~Process(es) for n~~Notification by the ~~of~~ vendor of vendor-identified incidents related to the products or services provided to the Responsible Entity that pose cyber security risk to the Responsible Entity~~events~~;

Order No. 829 Citation	Directive / Guidance	Resolution
		~~1.4.1.~~1.2.2. Coordination of responses to vendor-identified incidents related to the products or services provided to the Responsible Entity that pose cyber security risk to the Responsible Entity; ~~1.4.2.~~1.2.3. ~~Process(es) for n~~Notification by vendors when ~~vendor employee~~ remote or onsite access should no longer be granted to vendor representatives; ~~1.4.3.~~1.2.4. ~~Process(es) for d~~Disclosure by vendors of known vulnerabilities; ~~1.4.4. Coordination of response to vendor-related cyber security incidents;~~ ~~1.4.5.~~1.2.5. ~~Process(es) for verifying~~Verification of software integrity and authenticity of all software and patches provided by the vendor ~~that are intended~~ for use in the BES Cyber System; and ~~1.4.6.~~1.2.6. Coordination of ~~remote access~~ controls for (i) vendor-initiated Interactive Remote Access, and (ii) system-to-system remote access with a vendor(s)~~; and Other process(es) to address risk(s) as determined in Part 1.1.2, if applicable~~. **Proposed CIP-013-1 Requirement R2** **R2.** Each Responsible Entity shall implement its supply chain cyber security risk management plan(s) specified in Requirement R1.

Order No. 829 Citation	Directive / Guidance	Resolution
P 46	The new or modified Reliability Standard should also require a periodic reassessment of the utility's selected controls. Consistent with or similar to the requirement in Reliability Standard CIP-003-6, Requirement R1, the Reliability Standard should require the responsible entity's CIP Senior Manager to review and approve the controls adopted to meet the specific security objectives identified in the Reliability Standard at least every 15 months. This periodic assessment should better ensure that the required plan remains up-to-date, addressing current and emerging supply chain-related concerns and vulnerabilities.	The directive is addressed in proposed CIP-013-1 Requirement ~~R2~~R3. **Proposed CIP-013-1 Requirement ~~R2~~R3** **~~R2~~R3.** Each Responsible Entity shall review and obtain CIP Senior Manager or delegate approval of ~~update, as necessary,~~ its supply chain cyber security risk management plan(s) specified in Requirement R1 at least once every 15 calendar months~~, which shall include:~~ ~~**2.1.** Evaluation of revisions, if any, to address applicable new supply chain security risks and mitigation measures; and~~ ~~**2.2.** Obtaining CIP Senior Manager or delegate approval.~~
p 47	Also, consistent with this reliance on an objectives-based approach, and as part of this periodic review and approval, the responsible entity's CIP Senior Manager should consider any guidance issued by NERC, the U.S. Department of Homeland Security (DHS) or other relevant authorities for the planning, procurement, and operation of industrial control systems and supporting information systems equipment since the prior approval, and identify any changes made to address the recent guidance.	The directive is addressed in proposed CIP-013-1 Requirement ~~R2~~ R3 ~~part 2.1~~ (shown above) and supporting guidance. **Proposed CIP-013-1 Rationale for Requirement ~~R2~~R3:** ~~Order No. 829 also directs that the~~Entities perform periodic assessment ~~"ensure that the required~~to keep plans ~~remains~~ up-to-date and, addressing current and emerging supply chain-related concerns and vulnerabilities~~" (P. 47)~~. Examples of sources of information that the entity could consider~~s~~ include guidance or information issued by: •NERC or the E-ISAC •ICS-CERT •Canadian Cyber Incident Response Centre (CCIRC)

Order No. 829 Citation	Directive / Guidance	Resolution
		~~*Technical Guidance and Examples*~~*Implementation Guidance* ~~document~~ developed by the drafting team and submitted for ERO endorsement includes example controls.
Objective 1: Software Integrity and Authenticity		
P 48	The new or modified Reliability Standard must address verification of: (1) the identity of the software publisher for all software and patches that are intended for use on BES Cyber Systems; and (2) the integrity of the software and patches before they are installed in the BES Cyber System environment.	The directive is addressed in proposed CIP-013-1 Requirement R1 Part 1.2.5 (discussed above) and CIP-010-3 Requirements ~~R3~~ R1 ~~and R5~~ Part 1.6~~5.1~~. ~~CIP-013-1 Requirement R3 applies to high and medium impact BES Cyber Systems.~~ The objective of verifying software integrity and authenticity is to ensure that the software being installed in the BES Cyber System was not modified without the awareness of the software supplier and is not counterfeit. **Proposed CIP-~~013~~010-~~1~~ 3 Requirement ~~R3~~R1** **R1.** Each Responsible Entity shall implement one or more documented process(es) that collectively include each of the applicable requirement parts in *CIP-010-3 Table R1 – Configuration Change Management*.~~Each Responsible Entity shall implement one or more documented process(es) for verifying the integrity and authenticity of the following software and firmware before being placed in operation on high and medium impact BES Cyber Systems:~~ **1.6.** For a change that deviates from the existing baseline configuration associated with baseline items in Parts 1.1.1, 1.1.2, and 1.1.5, and when the method to do so is available to the Responsible Entity from the software source: **1.6.1.** Verify the identity of the software source; and

Order No. 829 Citation	Directive / Guidance	Resolution
		1.6.2. Verify the integrity of the software obtained from the software source.~~Operating System(s);~~ ~~**3.1.** Firmware;~~ ~~**3.2.** Commercially available or open-source application software; and~~ ~~**3.3.** Patches, updates, and upgrades to 3.1 through 3.3.~~ ~~**Proposed CIP-013-1 Requirement R5**~~ ~~**R5.** Each Responsible Entity with at least one asset identified in CIP-002 containing low impact BES Cyber Systems shall have one or more documented cyber security policies, which shall be reviewed and approved by the CIP Senior Manager or delegate at least once every 15 calendar months, that address the following topics for its low impact BES Cyber Systems:~~ ~~**5.1.** Integrity and authenticity of software and firmware and any patches, updates, and upgrades to software and firmware; and...~~
Objective 2: Vendor Remote Access to BES Cyber Systems		
P 51	The new or modified Reliability Standard must address responsible entities' logging and controlling all third-party (i.e., vendor) initiated remote access sessions. This objective covers both user-initiated and machine-to-machine vendor remote access.	The directive is addressed by proposed CIP-~~013~~005-~~1~~6 Requirement ~~R4~~ R2 Parts ~~4.1~~2.4 and ~~4.2~~2.5. The objective is to mitigate potential risks of a compromise at a vendor during an active remote access session with a Responsible Entity from impacting the BES.~~ and Requirement R5 Part 5.2. Requirement R4 applies to high and medium impact BES Cyber Systems.~~

Order No. 829 Citation	Directive / Guidance	Resolution
		~~Requirement R5 applies to low impact BES Cyber Systems.~~ The objective of Requirement R2 Part 2.4 is for entities to have visibility of active vendor remote access sessions (including Interactive Remote Access and system-to-system remote access) that are taking place on their system. The obligation in Part 2.4 requires entities to have a method to determine active vendor remote access sessions. The objective of Requirement R2 Part 2.5 is for entities to have the ability to rapidly disable active remote access sessions in the event of a system breach. **Proposed CIP-~~013~~005-~~1~~ 6 Requirement ~~R4~~R2** **R2.** Each Responsible Entity shall implement one or more documented processes that collectively include the applicable requirement parts, where technically feasible, in CIP-005-6 Table R2 –Remote Access Management.~~Each Responsible Entity shall implement one or more documented process(es) for controlling vendor remote access to high and medium impact BES Cyber Systems. The process(es) shall provide the following for (i) vendor-initiated Interactive Remote Access and (ii) system-to-system remote access with a vendor(s)~~: ~~**4.1.** Authorization of remote access by the Responsible Entity;~~ ~~**4.2.** Logging and monitoring of remote access sessions to detect unauthorized activity; and~~ ~~**4.3.** Disabling or otherwise responding to unauthorized activity during remote access sessions.~~

Order No. 829 Citation	Directive / Guidance	Resolution
		2.4 Have one or more methods for determining active vendor remote access sessions (including Interactive Remote Access and system-to-system remote access). **2.5** Have one or more method(s) to disable active vendor remote access (including Interactive Remote Access and system-to-system remote access). ~~**Proposed CIP-013-1 Requirement R5**~~ ~~**R5.** Each Responsible Entity with at least one asset identified in CIP-002 containing low impact BES Cyber Systems shall have one or more documented cyber security policies, which shall be reviewed and approved by the CIP Senior Manager or delegate at least once every 15 calendar months, that address the following topics for its low impact BES Cyber Systems:~~ ~~**5.2.** Controlling vendor-initiated remote access, including system-to-system remote access with vendor(s).~~
P 52	In addition, controls adopted under this objective should give responsible entities the ability to rapidly disable remote access sessions in the event of a system breach.	The directive is addressed by CIP-005-6 Requirement ~~R4~~ R2 Part ~~4~~2.~~3~~ 45 (above) ~~and Requirement R5 Part 5.2 (above)~~.
Objective 3: Information System Planning and Procurement		
P 56	As part of this objective, the new or modified Reliability Standard must address a responsible entity's CIP Senior Manager's (or delegate's) identification and documentation of the risks of proposed information system planning and system	The directive is addressed in proposed CIP-013-1 Requirement R1 Part 1.1 (shown above).

Order No. 829 Citation	Directive / Guidance	Resolution
	development actions. This objective is intended to ensure adequate consideration of these risks, as well as the available options for hardening the responsible entity's information system and minimizing the attack surface.	
Objective 4: Vendor Risk Management and Procurement Controls		
P 59	The new or modified Reliability Standard must address the provision and verification of relevant security concepts in future contracts for industrial control system hardware, software, and computing and networking services associated with bulk electric system operations. Specifically, NERC must address controls for the following topics: (1) vendor security event notification processes; (2) vendor personnel termination notification for employees with access to remote and onsite systems; (3) product/services vulnerability disclosures, such as accounts that are able to bypass authentication or the presence of hardcoded passwords; (4) coordinated incident response activities; and (5) other related aspects of procurement. NERC should also consider provisions to help responsible entities obtain necessary information from their vendors to minimize potential disruptions from vendor-related security events.	The directive is addressed in proposed CIP-013-1 Requirement R1 Part 1.2 (shown above).